Privacy Office

Report to Congress

April 2003 – June 2004

Homeland Security

Privacy and Protecting Our Homeland

"To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy."

The National Strategy for Homeland Security

Preserving our Freedoms, protecting America … We secure our homeland.

Objective 7.1: Protect confidentiality and data integrity to ensure privacy and security.

Protecting vital and sensitive information, thus ensuring the privacy of American citizens, is important to the safety of the Nation. We will ensure the technologies employed sustain, and do not erode, privacy protections relating to the collection, use and disclosure of personal information. We will eliminate inappropriate access to confidential data to preserve the privacy of Americans. We will maintain an appropriate balance between freedom and safety consistent with the values of our society.

U.S. Department of Homeland Security Strategic Vision

U.S. Department of Homeland Security
Privacy Office
Washington, DC 20528

Homeland Security

Honorable Members of Congress, fellow Americans, and neighbors around the globe:

It is my great honor to submit to the United States Congress a report on the first year of the operations of the Privacy Office at the Department of Homeland Security. I am particularly pleased to have held this role during the Department's first year at a time when, under the tremendous leadership of Secretary Tom Ridge, we seized the opportunity to promote new and lasting awareness of the responsible handling of personal information about citizens and visitors to our country.

The responsible stewardship of personal information is fundamental to the Department's successful achievement of its mission. This mission is not only to protect our people and our homeland; it is to protect our way of life. Personal privacy is central to that way of life. Privacy is a core value, universally recognized, and a value long recognized in American law and jurisprudence. Because privacy is so essential to our way of life we recognize that the protection of privacy, of the very dignity and autonomy of the individual, is not a value that can be added on to this or any other organization as an afterthought. Thus, I am so pleased that the Privacy Office has been operational within the Department of Homeland Security from its earliest days. We will continue to work to ensure that privacy is woven into the very fabric of this organization as a guiding principle and value.

Our accomplishments over the first year of the Department's history are a demonstration of Congressional and Presidential foresight in embedding privacy protection into the security mission of the Department of Homeland Security. I believe that our work is testament to the commitment of our leadership and dedicated staff throughout the agency.

I also believe we have made our influence felt outside the walls of the Department, both at home and abroad, by listening to privacy concerns and by responding in positive, constructive ways. This will continue to be accomplished by consulting closely with Congress, with our colleagues across government, with representatives of the private sector, and with our counterparts in the international community.

I look forward to continuing to work within the Department to build the Department of Homeland Security into a model for the protection of our homeland and also for the protection of the privacy of all people.

Humbly submitted,

Nuala O'Connor Kelly

Nuala O'Connor Kelly
Chief Privacy Officer

Privacy -- Part of the Department's Mission

"We must and we will be careful to respect people's privacy . . . . Terrorists hide among us and use our freedom against us, but they will find fewer places to hide if we provide accurate, verifiable, timely information to the people charged with protecting us.

Fear of government abuse of information, like fear of terrorism, is understandable. But we cannot let it stop us from doing what is right and responsible. The antidote to this fear, I might add, is an open, fair, and transparent process that guarantees the protection and privacy of that data.

In addition to the federal privacy safeguards already on the books, the Department of Homeland Security will have its own privacy officer. . . . That individual will be involved from the very beginning with every policy initiative and every program initiative that we consider, to ensure that our strategy and our actions are consistent with the individual rights and civil liberties protected by the Constitution.

We'll work together to ensure that our programs appropriately use information, protect it from misuse, and discard it when it is of no further use. It is, however, critical that information be accurate, comprehensive and up-to-date."

Tom Ridge
Secretary
U.S. Department of Homeland Security

"Privacy is a value that must be embedded in the very culture and structure of the organization. I know that we can and will succeed in this – because our leadership and our employees believe in and act on this value – for themselves, their neighbors, and their families – each day."

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security

TABLE OF CONTENTS

APPENDICES

For an online copy of this report, log on to www.dhs.gov\privacy.

THE DEPARTMENT OF HOMELAND SECURITY
PRIVACY OFFICE
REPORT TO CONGRESS
APRIL 2003 - JUNE 2004

PRIVACY OFFICE STRUCTURE

Establishment of the Privacy Office

The DHS Privacy Office is the first statutorily required comprehensive privacy operation at any federal agency. It operates under the direction of the Chief Privacy Officer, who is appointed by the Secretary. The DHS Privacy Office serves as the steward of Section 222 of the Homeland Security Act of 2002, and has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act of 2002, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personal and Departmental information. The Privacy Office ensures that appropriate access to or withholding of information is consistent with these statutes as well as with the Vision, Mission, and Core Values of DHS.

Privacy Protection is an Integral Part of the DHS Security Mission

Contributing to all of the Department of Homeland Security's Strategic Goals, the Privacy Office implements the Guiding Principles of the Department to defend and protect the individual rights, liberties, and the information interests of our citizens, residents and visitors. Secretary Ridge, in anticipation of his appointment of Chief Privacy Officer Nuala O'Connor Kelly, announced his vision of the mission of the Privacy Office, explaining that the Privacy Office "will be involved from the very beginning with every policy initiative and every program initiative that we consider," to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books, but also "with the individual rights and civil liberties protected by the Constitution."

Specific Privacy Office Responsibilities

The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the Privacy Act of 1974, the Freedom of Information Act, and the completion of Privacy Impact Assessments on all new programs, as required by the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. The Privacy Office also is statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. Further, the Privacy Office is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

Statutory Duties of the Chief Privacy Officer

The responsibilities of the Chief Privacy Officer of the Department of Homeland Security as set forth in Section 222 of the Homeland Security Act of 2002, are to assume primary responsibility for privacy policy, including –

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.

The Homeland Security Act of 2002, Pub. L. No.107-296, Title II, § 222, 116 Stat. 2155.

Additional Responsibilities

The work of the Privacy Office includes not only the statutory privacy work required under U.S. law, but also Freedom of Information Act (FOIA) compliance for the Department. This additional responsibility for FOIA compliance was delegated to the Privacy Office by the Secretary during the summer of 2003, in recognition of the close connection between privacy and disclosure laws, and the functional synergies of the work of more than 430 Privacy Act and FOIA specialists across the Department. Those specialists now work on Privacy Act and FOIA compliance matters under policy guidance from the Chief Privacy Officer.

Since the Department's focus is necessarily international as well as domestic, the Privacy Office addresses cross-border privacy issues. Compliance responsibilities of the Privacy Office include oversight of implementation of international arrangements that facilitate DHS program goals. Additionally, the Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 180,000 employees and new hires.

DHS Privacy Staff

The Privacy Office's initial staffing at DHS headquarters has been recruited to functionally address major DHS privacy and transparency responsibilities as follows:

- Chief Privacy Officer;
- Chief of Staff and Director, International Privacy Policy;
- Chief Counsel for the Privacy Office (Office of the General Counsel);
- Director, Departmental Disclosure and FOIA;
- Director, Privacy Technology; and
- Director, Privacy Compliance.

Additionally, more than 430 Privacy and FOIA specialists throughout the Department contribute to compliance efforts and implement DHS privacy and FOIA policy each day.

Finally, three Privacy Officers, with dual reporting relationships to the Chief Privacy Officer and to their offices, have been appointed to the following areas: the US-VISIT Program, the National Cyber Security Division (within the Information Analysis and Infrastructure Protection Directorate) and the Transportation Security Administration (TSA).

Privacy Office Headquarters Staff Responsibilities

Chief Privacy Officer. The Chief Privacy Officer (CPO) is responsible for policy oversight and implementation of the Privacy Act and FOIA, for office direction and policy creation, and for initiating and directing inquiries and investigations in cases of alleged privacy violations or misuse of personal information.

Chief of Staff and Director, International Privacy Policy. The Chief of Staff and Director, International Privacy Policy, coordinates implementation of policy direction and office management under the CPO and serves as senior advisor to the Department on international privacy frameworks and policies, advises on negotiations and external relationships with the European Union and other global regions, and handles international privacy matters and inquiries.

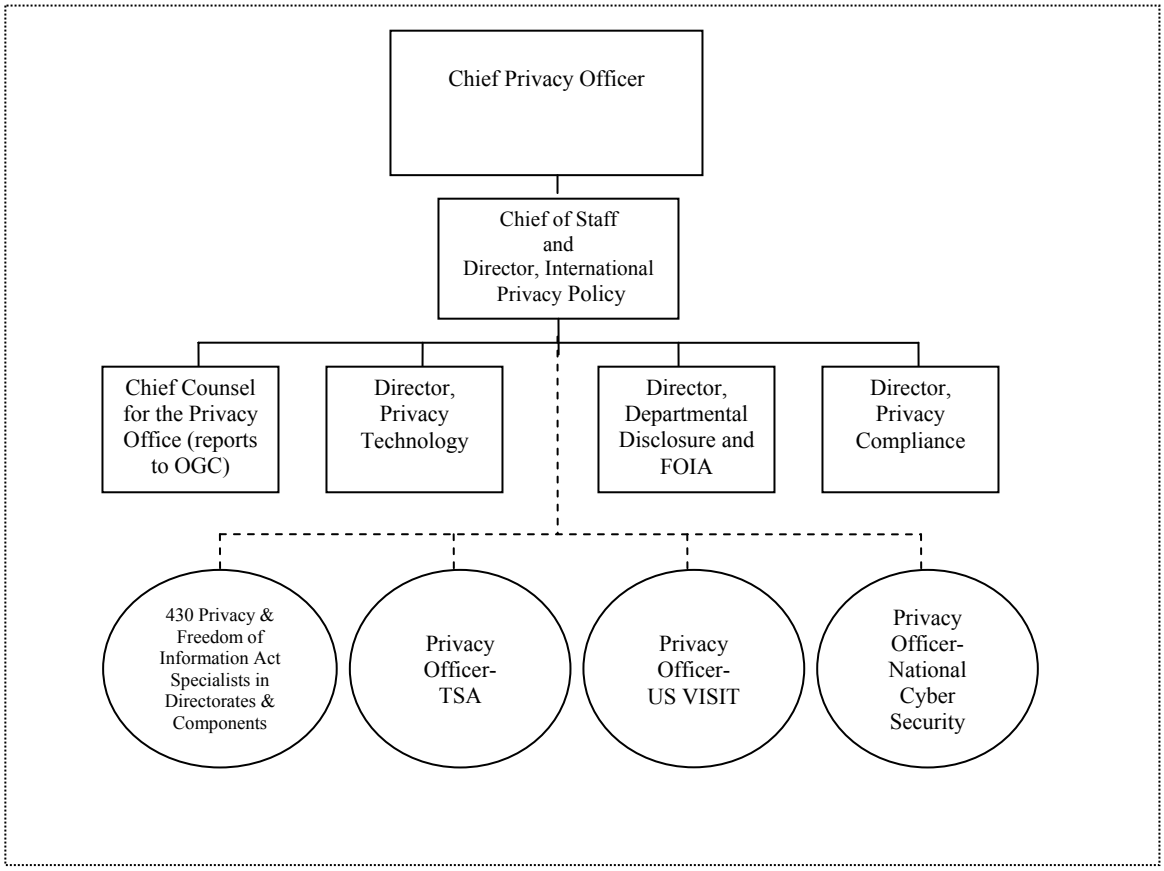
Chief Counsel for the Privacy Office. The Chief Counsel provides legal advice on the full range of issues concerning information disclosure and privacy law and reviews Privacy Office documents for legal sufficiency and statutory compliance. Embedded within the Privacy Office, the Chief Counsel is part of the DHS Office of the General Counsel, and reports to the Division of General Law.

Director, Departmental Disclosure. The Director, Departmental Disclosure, oversees FOIA and Privacy Act disclosure compliance across the Department and directs Privacy Act and FOIA disclosure policy and is charged with creating a Privacy Act/FOIA appeals function at DHS headquarters.

Director, Privacy Technology. The Director, Privacy Technology, advises Departmental leaders on privacy-sensitive technology development, evaluates new technologies for privacy impact, enforces privacy policies on DHS websites and other citizen-facing communications, and serves as a liaison to the Chief Information Officer's Office, the Directorate for Information Analysis and Infrastructure Protection, and the Directorate of Science and Technology, in particular.

Director, Privacy Compliance. The Director, Privacy Compliance, assures compliance with privacy policy including privacy impact assessment requirements, by benchmarking the various components' privacy education and training, protocols, and protections, educates employees and leaders on best practices, and performs an internal audits function on privacy compliance.

DHS Privacy Office Organizational Chart 2004



Note: In FY 2004, the DHS Privacy Office has been staffed with the direct reports shown above, as well as a number of contractors performing administrative operational functions and supporting the Privacy Act/FOIA function, as well as several short-term detailees from other directorates who serially provided FOIA support. We also have relied upon a number of detailees from other Federal agencies, including the Departments of Justice, Agriculture, and Commerce, for additional privacy program support.

Summary

This Report on Department of Homeland Security privacy activities, covering the period from the creation of the Privacy Office until July 2004, demonstrates that, through the establishment and functionality of the operations of the DHS Privacy Office, we are working to "operationalize" privacy awareness and best practices throughout DHS.

We have made privacy an integral part of DHS operations by working side-by-side on DHS initiatives with the senior policy leadership of the various directorates and components of DHS and with program staff across the Department. As a result, the Privacy Office has been able to embed privacy values into the culture and structure of DHS in order to ensure that, as DHS programs move forward to implementation, they have been carefully and thoroughly analyzed for their impact on personal privacy and, once implemented, are effective in protecting the homeland while protecting personal privacy.

The DHS Privacy Office is pleased to share with Congress and the American people the policy and legal architecture applicable to DHS to safeguard individual privacy. This report contains the Privacy Office's milestones during the past fourteen months toward satisfying the objectives of those laws and the development of DHS privacy policy, pursuant to Section 222 of the Homeland Security Act of 2002.

KEY PRIVACY FRAMEWORKS

The Privacy Act of 1974

One of the primary laws supporting the mission of the DHS Privacy Office is the Privacy Act of 1974. The Privacy Act, 5 U.S.C. § 552a, provides a code of fair information practices that governs the collection, maintenance, use, and dissemination of personal information by federal agencies. Emanating from concerns about the ability to aggregate personal information -- due, in part, to advances in technology -- this law provides substantial notice, access, and redress rights for citizens and legal permanent residents of the United States whose information is held by the executive branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information and carefully prescribed limits on the release of that information. The law also provides the right of access to one's own records, the right to know other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy or disclosure of those records. The Privacy Act is our country's articulation of Fair Information Principles; the Act both protects the information of our citizens and also provides our citizens rights to access that data.

Freedom of Information Act

The Freedom of Information Act, 5 U.S.C. § 552, embodies the principle that persons have a fundamental right to know what their government is doing. Our government and our agency are grounded on principles of openness and accountability, tempered, of course, by the need to preserve the confidentiality of sensitive personal, commercial, and governmental information. The Freedom of Information Act is the primary statute that attempts to balance these countervailing public concerns. A robust FOIA/PA program is a critical part of any agency's fundamental processes; it helps to provide assurance to the public that, in pursuing its mission, an agency will also pursue balanced policies of transparency and accountability while preserving personal privacy. The federal government will spend hundreds of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests. Our agency alone has over 430 staff members across the Department who work full or part-time on FOIA and Privacy Act issues.

The E-Government Act of 2002

Specific portions of the E-Government Act of 2002 are particularly relevant to the Privacy Office's function. Section 208 of the E-Government Act mandates Privacy Impact Assessments for all Federal agencies when there are new collections of, or new technologies applied to, personally identifiable information. In September 2003, the Office of Management and Budget released its guidance under Section 208. These requirements are further articulated in Section 222 of the Department's organic statute.

Privacy Impact Assessments, or PIAs, are a third pillar of the privacy framework at the federal level, and reflect the growing reliance on technology to move data -- both in government spaces and on the Internet. With the addition of the privacy provisions of the E-Government Act to existing privacy protections, individuals now benefit from a comprehensive framework within which government considers privacy in the ordinary course of business.

The Act and underlying guidance synthesize numerous prior statements and guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides direction on the content of privacy policies and on the machine-readability of privacy policies.

The Act and guidance outline the parameters for privacy impact assessments. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the privacy of individuals . . . before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness of the impact on the individual and the purpose of the collection, both by those seeking to collect the data and those whose data is collected. The Privacy Office is working with privacy practitioners across the agency, as well as with the Chief Information Officer (CIO), legal, and budget office teams to implement a rigorous PIA process, whereby every new technology use or acquisition is subject to a PIA.

A Unified Privacy Architecture for the Government Space

Under the Privacy Act, in concert with FOIA and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them. A robust FOIA and Privacy Act program is imperative to provide the public with assurances that any information DHS collects is being maintained consistent with all requirements.

PRIVACY POLICY DEVELOPMENT

The Chief Privacy Officer of the Department of Homeland Security's responsibilities, as set forth in Section 222 of the Homeland Security Act, are "to assume primary responsibility for privacy policy. . .

Section 222,
Homeland Security Act of 2002

"*We at Homeland Security are forging a new way forward. This new way forward will require clear policies, definite policies, and intelligent choices about the responsible use of information by our government and by the private sector."*

Nuala O'Connor Kelly
Chief Privacy Officer
October 30, 2003

Pragmatic Optimism and Practical Privacy Objectives

Pragmatic optimism has marked the approach to building privacy awareness and compliance into the culture, security mission, policies, practices and aspirations of the Department of Homeland Security. To that end, no one has been a greater supporter, in word and deed, than Secretary Tom Ridge. His active support for the independence of the Chief Privacy Officer and the establishment of a functioning Privacy Office, with a dedicated budget and strong input and influence on shaping DHS programs, has set the bar high for expectations of privacy compliance throughout the Department. Under Secretary Ridge and Deputy Secretary Jim Loy, the entire leadership team of the Department has embraced the value of privacy as an integral DHS cultural value and as an important sign of our respect for DHS employees, American citizens and legal permanent residents, and visitors to our welcoming nation.

In building privacy awareness into the fabric of DHS, three key challenges were identified in this initial year: (1) operationalizing privacy throughout DHS; (2) the need to address use of private sector data; and (3) international cooperation.

Operationalizing Privacy throughout the Department of Homeland Security

In the first year of the Privacy Office, much time was given to what has been described internationally as "practical privacy." With the merger of 22 existing agencies to form a unified DHS, time was necessarily spent assessing current privacy and government transparency operations in the legacy component agencies and formulating a practical way forward for operationalizing privacy throughout the Department. The path chosen was to identify significant functional privacy areas and to assemble a seasoned team of privacy professionals to fill senior positions that addressed those functional objectives and to provide leadership at the Departmental level. To that end, as reflected in the earlier

portions of this Report, the Chief Privacy Officer determined the need for functional expertise to assist the Department with privacy technology, privacy compliance, privacy policy, disclosure policy and international privacy policy.

In operationalizing privacy, the Privacy Office reports directly to the Secretary and works collaboratively with senior policy leadership of the various agencies and directorates of the Department, as well as with more than 430 Privacy Act and FOIA team members, Privacy Officers, and other operational staff across the Department. Additionally, the DHS Privacy Office works collaboratively with Privacy Officers across the Administration and with privacy leaders at the Office of Management and Budget (OMB) and the Department of Justice, to consult on best practices and polices for agency privacy offices.

The Privacy Office works closely with the DHS General Counsel and the Chief Information Officer to ensure that the mission of the Privacy Office is reflected in all DHS initiatives. The especially close working relationship of the Privacy Office and the Office of the General Counsel, led by General Counsel Joe Whitley, enables DHS to meet its security mission, while protecting personal information by being fully counseled on the legal and regulatory ramifications of U.S. privacy laws and their interrelationship with statutes and proposed legislation affecting homeland security. And, of course, we also work in concert with the Department's Office for Civil Rights and Civil Liberties on matters of mutual interest and concern.

Much of this Report addresses operationalizing privacy in a new and changing organization. This is a challenging mission, and DHS is committed to complying with applicable privacy laws, best practices, and fair information principles. The Privacy Office has made significant progress in creating a strong foundation of privacy protections throughout DHS programs, technologies, and policies in our first year. We look forward to continuing the process of educating the more than 180,000 DHS employees on these matters.

One of the ongoing challenges that has persisted this year and will continue next year is everyday compliance with good privacy practices, including the need for privacy policies on DHS websites, the need to comply with all privacy laws. This compliance includes not just the Privacy, FOIA and E-Government Acts, but also the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and other pertinent laws, if they are applicable to DHS programs or information sharing, including concerning employee information. The need for education and training is made all that much more clear by these examples and other areas, such as the legal mandate for privacy impact assessments, to educate and remind our employees on compliance requirements and due care.

Also in this first year, in terms of emphasis and available staff resources, a great deal of Privacy Office review and assistance has been given to programs emerging from the Directorate of Border and Transportation Security (BTS), in particular, from the Transportation Security Administration and Customs and Border Protection components, to assist with the immediate mission of securing and facilitating travel and borders. Under Secretary Asa Hutchinson and Assistant Secretary Stewart Verdery have, in particular,

been active leaders and partners in making sure that BTS programs reflect the security and privacy protection objectives of the Department.

Approximately 120,000 of DHS's more than 180,000 employees work within the BTS Directorate. Their efforts are on the front line of developing programs and protocols for better securing our homeland from terrorists and others who seek to threaten the freedoms of our citizens and those who visit what is, and has always been, our welcoming nation. To that end, the Privacy Office played an integral advisory role concerning all phases of the US-VISIT program and proposed CAPPS II program. In response to operational factors and internal and public comments concerning CAPPS II, DHS has redesigned an automated advanced screening program and recently announced a new domestic program, Secure Flight. The Privacy Office has provided assistance and collaboration on many other border and transportation security programs, including those related to screening of hazardous materials drivers and registered travelers, to ensure that privacy considerations and protections for all individuals are built into DHS programs.

Use of Private Sector Data

One of the most important public policy challenges facing not only DHS but also the federal government as a whole is the sharing of personal information between the public and private sector. This issue resonates with American citizens, foreign visitors, political leaders both at home and abroad, and within DHS where the responsible handling of personal information is critical to the successful performance of our mission.

The Privacy Office's examination of the events surrounding alleged privacy violations concerning voluntary transfers of passenger name record (PNR) data from the private sector to the government is one example of why it is so important to have in place all necessary protections for personally-identifiable information. Even when actual Privacy Act violations are not found, it is nevertheless important that clear rules be in place to ensure that information sharing is done in a legitimate, respectful, and limited way. Going forward, the challenge facing the Privacy Office is to carefully navigate between the privacy and security concerns inherent in information sharing and to build a consensus on the responsible use of private sector data so that we can further our efforts to enhance homeland security while maintaining robust protections for personal privacy.

To that end, the Privacy Office has been engaged in dialogues with many private sector groups, encouraging them to develop their own internal guidelines as well as recommendations for "best practices" for public-private data sharing so that the Privacy Office can obtain a range of views and input on this matter. The appropriate use of private sector information by DHS is also one of the major issues that the ***Data Integrity, Privacy, and Interoperability Advisory Committee***, now being formed, will consider as a first order of business. That Committee will reflect the diverse viewpoints of all sectors -- business, academia, privacy advocacy, technology and security specialists, and policy generalists. (See Appendix I)

A related topic discussed further below is "data mining." Technology has broadened exponentially our ability to extract information from data. It is important that we bring fair information principles to the quest for knowledge from existing and new data

sources in order to legitimatize our efforts and build a consensus on respectful use of the information that is available to us.

Through the issuance of public reports, the Privacy Office has and will continue to share with Congress and the public information regarding investigations and conclusions about data sharing and data mining.

International Cooperation

Since the Department's work affects not only citizens but also visitors to our country and persons throughout the world, the Privacy Office's work is necessarily international as well as domestic. A key focus of the Privacy Office's work in this first year has been to engage data protection authorities and privacy and security advocates internationally. In these efforts, of course, we ensure interagency policy coordination.

Outreach

Significant efforts have been spent on outreach by the Chief Privacy Officer and the Chief of Staff and Director for International Privacy Policy. The Privacy Office has met with Data Protection and Privacy officials from Canada, the European Union, Australia, Asia, and Latin America in 2003-2004. The Chief Privacy Officer has testified before a committee of the European Parliament and was a speaker before the International Association of Data Protection and Privacy Commissioners in 2003. In all cases, the purposes of these interactions have been, in part, to better explain the privacy framework that exists in the United States, which protects the privacy of personal information when it is collected, used, shared and retained by the U.S. government.

Our dialogues have resulted in the beginnings of greater understanding of the U.S. system, but have also revealed a nearly universal misconception that the United States has no privacy framework that might be viewed as consonant with those of other countries. In fact, this is not the case, particularly with respect to privacy laws applicable to the public, governmental sphere – the Privacy Act of 1974 that has been in existence and use for 30 years that provides access and redress rights to all individuals with respect to their own personal information, and the Freedom of Information Act that provides access to government records including personal information, and the E-Government Act of 2002 that requires Privacy Impact Assessments of all new technologies and government databases that collect or store personal information about any individual, whether a U.S. citizen or not. (See above, *Key Frameworks Enforced by the Privacy Office*)

The fact that our most basic and overarching implementation of fair information principles is embodied in the Privacy Act of 1974 and, according to a plain reading of the statutory language, protects only the privacy interests of U.S. citizens and permanent residents whose information is collected by the U.S. government, has presented a challenge in our international dialogues. Global neighbors communicated their perception that the U.S. interest in privacy protection and privacy rights may be parochial, isolated to Americans only, fueling the misperception of U.S. non-comparability with basic information privacy protections afforded in many other regions of the world to any individual, regardless of status. Arguably, this was one of the most serious points of

discussion and concern from the European side during the recently concluded negotiations on permitting the sharing of Passenger Name Records with DHS's Customs and Border Protection component to assist in advance passenger screening of travelers flying between the U.S. and the European Union.

Common Dialogue with Shared Privacy Principles

Privacy professionals and officials the world over, share a common interest in assuring public trust in government operations by encouraging government transparency, as well as respect for fair information principles in handling personal information, such as collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, participation and accountability. Sometimes these concepts are articulated using different titles, but the notions remain substantially similar. An important bridge in communications across borders, where legal systems may differ significantly and, thus, also the presentation of privacy protections, are common understandings about guidance provided by voluntary, internationally recognized privacy principles.

To that end, the Organization for Economic Cooperation and Development's (OECD's) Privacy Principles, long standing since the early 1980s (shaped, in part, by the fair information principles of the U.S. Privacy Act of 1974), and the emerging principles from the Asia-Pacific Economic Cooperation (APEC) concerning data handling in a networked world, all are important in promoting cross-border cooperation. They provide the vehicles and needed flexibility for recognizing the privacy protections of different economies and regions that reflect differences in culture, political structures and legal systems, but share a common foundation grounded on accepted privacy principles. To this end, DHS participation in multilateral groups that consider international privacy principles and their applications is critical in developing working relationships and international cooperation on a variety of homeland security measures.

One example of the potential for employing international privacy principles as a bridge in dialogues among global neighbors and security partners has been in the context of joint work by the International Civil Aviation Organization (ICAO) and the OECD's Working Group on Information Security and Privacy (WPISP). The effort centers on developing an international information-sharing system that will facilitate real-time sharing of data on lost or stolen passports. Use of fraudulent or lost and stolen passports by terrorists and by serious transnational criminals threatens the security of America and our global neighbors. The United States, and DHS, in particular, supports this joint work of ICAO and the OECD, which promotes the use of OECD Privacy Principles as a framework for dialogue and policy guidance from the OECD-WPISP on how to design the information-sharing system's architecture to include privacy enhancing protections while effectively achieving needed homeland security controls. The Privacy Office's Chief of Staff and Director of International Privacy Policy has been the U.S. Delegation spokesperson at the OECD WPISP on this initiative, supporting U.S. efforts in many multilateral settings and in bilateral relationships for Enhanced International Travel Security programs.

Additional areas where dialogues center on accepted international privacy principles, rather than on legal differences of countries, include the use of biometrics and

new technologies in an array of homeland security enhancing programs and applications. These include dialogues within the International Standards Organization, the OECD, and ICAO, among other multilateral venues.

Engaging Data Protection Authorities Internationally

An important focus of the Privacy Office's work has been to engage the data protection authorities internationally. Our office has participated in meetings of the International Data Protection and Privacy Commissioners, although our office is not recognized at this time as an accredited data protection authority.

The Privacy Office has, however, submitted an application for and been approved as an official "Observer" to the International Data Protection and Privacy Commissioners Conference, in order to participate in both open and closed discussions among governmental data protection authorities from around the world on the serious issues relevant to protecting individual privacy. Today, these issues often focus on information privacy and the use of emerging technologies in a networked world for homeland security and other data sharing purposes.

The acceptance of this application represents the first official U.S. government representation within this body, notwithstanding wide participation from countries from every region in the world. We believe it is in the interest of the American people we serve, and would assist us in addressing concerns of visitors and building bonds with global neighbors, to be at the table as listeners, learners, participants, partners and advocates. We are confident that the important dialogues within this body will increase opportunities for international cooperation and will demonstrate a unified commitment world-wide to protecting individual freedoms.

Other International Privacy Issues

The Privacy Office has actively engaged in international discussions and participated in domestic and international workshops on the design of effective Privacy Notices, including short-layered privacy notices. These discussions broadly involved data protection authorities, consumer and privacy advocates, and multinational businesses representatives from the United States, Europe, and Australia.

In addition to domestic discussions on the use of technologies in a privacy enhancing, rather than an intrusive, manner, the Privacy Office has participated in discussions on a range of technology issues with other data protection staff and privacy advocates from Europe and Latin America and the United States through the International Working Group on Data Protection in Telecommunications. These discussions span technologies such as RFIDs to biometrics and many other issue areas.

Other issues that come up in the context of international privacy issues internally for review and in the context of international outreach include G-8 proposals that include a recognition of the need for privacy reviews in the design and implementation of the proposals, issues concerning maintaining data integrity and, generally, the protection of personal information in a cross-border context.

Compliance

Compliance responsibilities of the Privacy Office include oversight of implementation of international arrangements that facilitate DHS program goals. These currently include the recently concluded U.S.-EU PNR Agreement and the US-EU Europol Agreement on Data Protection.

The Privacy Office played a significant role within DHS during the US-EU PNR Agreement negotiations, by providing advice on fair information practices, and European Data Protection law and its implementation. In connection with those negotiations, the Chief Privacy Officer and the Director for International Privacy Policy traveled with the U.S. team to facilitate dialogues and information exchanges about U.S. privacy practices with European Commission members and staff, members of the European Parliament, U.S. Embassy staff in Europe doing outreach from their posts, advocacy groups and foreign press.

Since the PNR Agreement was signed in May 2004, the Privacy Office has proactively assisted with implementation efforts, including posting a Privacy Statement concerning the Agreement on its website, www.dhs.gov/privacy, composing Frequently Asked Questions for further notice to the public and suggested privacy statements that might be used by airlines, travel industry representatives, and central reservation systems. Internally, the Privacy Office has a role in auditing compliance with the terms of the Agreement and Undertakings. The Privacy Office will facilitate the annual joint review of progress made on implementing the PNR Agreement and Undertaking representations.

Under the terms of the Undertakings, as a result of concerns expressed about non-citizens or non-residents not having the same privacy protections for information collected by the U.S. Government that are extended under the Privacy Act to Americans citizens and permanent residents, the Privacy Office itself will function as a clearinghouse for international correspondence or complaints related to the PNR Agreement, and will provide a special appeals function, as well, at the Departmental level for complaints and questions. A foreign national may contact Customs and Border Protection and the Privacy Office directly or through their member country data protection commissioner and priority review will be given to such complaints/contacts. While this feature is specific to the U.S. – EU PNR Agreement, within the Privacy Office we look forward to working with Data Protection Authorities from any region in assisting them help their citizens or residents pursue reviews in connection with privacy concerns or possible privacy violations related to DHS activities.

PRIVACY AND TECHNOLOGY

". . . (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;"

Section 222 (1), The Homeland Security Act of 2002

The Department constantly seeks to leverage the newest technology tools in the War on Terrorism. New data technologies can support new ways of looking at existing information and can offer new opportunities for collecting and analyzing information. When so many of these data collections impact personal information, privacy protections are an essential element of such technological tools. As a result, ensuring that privacy is part of the core architecture of new technologies is one of the key missions of the DHS Privacy Office.

In fact, the very first task for the DHS Privacy Officer enumerated in Section 222 of the Homeland Security Act of 2002 is to "assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." As a result of this mandate, the Privacy Office has been involved from the very beginning in numerous DHS initiatives that apply technology to the collection of personally identifiable data.

A primary goal of the Privacy Office is to raise the level of privacy awareness and develop active communications among scientists, engineers, and other technicians who are investigating options and crafting proposals for DHS's technological response to terrorism. The Privacy Office has accomplished this by working with the science and technical organizations across the Department as well as with the private sector.

By examining technologies generally, independent of any particular application within the Department, the DHS Privacy Office is able to bring a privacy framework to the Department for major areas of technology that can be used Department-wide. This "outside look" at specific technologies also streamlines the process of ensuring that as various organizations approach the same technology across different applications, the issues that are raised by that common technology are addressed from a single perspective. In consequence, the Privacy Office can ensure that technology is consistently implemented and structured to account for issues of privacy protection and awareness.

The following are some specific technologies that the DHS Privacy Office has actively examined:

Biometrics

One tool that appears increasingly promising for use in securing the homeland is biometrics. Biometrics refers to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. The Department is leading the way in exploring the use

of these technologies for identification purposes, and the Privacy Office has ensured its place at the table so that privacy concerns can be addressed at all points along the development and implementation phases.

One of the primary programs collecting and using biometrics is the US-VISIT Program. The Chief Privacy Officer is a permanent member of the oversight board for the US-VISIT Program and reviewed and assisted in "baking in" privacy protections to the architecture of the program. The US-VISIT program is discussed further at Part 5 of this Report. (See also the US-VISIT Privacy Impact Assessment at Appendix F.)

From its inception, the DHS Privacy Office has been an active participant in a series of different biometrics committees and working groups at various levels of government and industry.

Biometrics Coordination Group

The DHS Privacy Office has been actively engaged in the "Biometrics Coordination Group" within the Department, which ensures that all biometrics work across all of DHS approaches the technology from a harmonized perspective and with awareness of each individual application of the technology.

National Science & Technology Council's Inter-Agency Working Group on Biometrics

The DHS Privacy Office is co-chair of the Social/Legal/Privacy subgroup of this Inter-Agency working group. In that role the Privacy Office is actively influencing governmental implementation of biometric technologies from a privacy protection perspective.

Biometrics Interoperability and Programs

The DHS Privacy Office is an active member of this interagency program to identify opportunities for focusing expertise from multiple agencies to benefit biometrics programs on a government-wide basis.

International Working Groups

Through its participation in groups such as INCITS (The International Committee for Information Technology Standards), ISO (The International Organization for Standardization), ICAO, the OECD's Working Party on Information Security and Privacy and other multilateral groups, the DHS Privacy Office is actively engaged internationally in the discussion of how biometric technologies and privacy protection considerations can best fit together. This is true particularly in the context of information sharing on lost and stolen passports and other programs for enhanced international travel security, including the development of machine readable passports that contain biometric identifiers.

Radio Frequency Identification Devices

RFID (Radio Frequency Identification Devices) are another technology series drawing significant attention from the Privacy Office. RFIDs have been defined as "an analog-to-digital conversion technology that uses radio frequency waves to transfer data between a moveable item and a reader to identify, track or locate that item."[1] The DHS Privacy Office has been actively engaged in many discussions regarding the use of RFID technologies across both government agencies and industry.

In the period covered by this report, the DHS Privacy Office participated in the Federal Trade Commission's workshop on RFID technology and also in a working group of the Center for Strategic and International Studies. Both of these events brought together members of federal government agencies, academicians, industry users, and researchers to examine how the technology operates and the related privacy and policy implications. As a result of these discussions, should RFIDs be proposed for use in connection with DHS programs, the Privacy Office will be better able to ensure that the technology is used in ways that enhance rather than erode privacy protections.

Internally, the Privacy Office has reviewed proposals for possible use of RFID technologies, including a piloted program at two airports to track baggage through the security process. The pilots tracked the movement of "things" rather than "people," in order to better enhance travel by making sure that the luggage of travelers reaches the correct airliner once any security check has been completed.

"Data Mining"

The term "data mining" has many connotations, not all of which are positive. One of the major goals of the Privacy Office is not only to build a consensus for arriving at a common meaning for this term within DHS, but also, more importantly, to arrive at a consensus on an appropriate policy for using databases – both public and private – to enhance the knowledge of personnel across DHS who are actively engaged in the War on Terrorism and serious crimes threatening the homeland, particularly in protecting our borders, ports and major infrastructures.

The Privacy Office has been engaged in this effort on a practical level. One definition of data mining recognizes the concept of "distributed data environments" – where data stays with the "owner," but queries are performed across the network where the data is stored. With the DHS Directorate of Science and Technology (S&T), the Privacy Office participated in a workshop concerning "distributed data environments," which also drew in representatives from the San Diego Supercomputer Center, from the private sector and from academic institutions. The focus of these and other discussions with DHS staff and academicians is to foster mutual understanding of privacy protection principles and strategies for those who are researching and developing distributed technology. The DHS

Privacy Office is also working with S&T on using distributed system architecture to enhance travel and travel document security from a privacy-centric perspective.

In this area, the Privacy Office has also taken specific steps to ensure that data mining programs that receive DHS funds conduct their activities with the utmost concern for personal privacy, and that they employ best practices regarding their use of personally identifiable information. To that end, the Privacy Office has undertaken a comprehensive review of the Multi-State Antiterrorist Information Exchange (MATRIX), a network of law enforcement databases that has received some DHS support through a cooperative agreement.

In the near future, the Privacy Office will issue a report assessing the benefits and deficiencies of MATRIX and the role of DHS in supporting the program. That report, like all of the activities of the Privacy Office, is motivated by the belief that building a privacy architecture on the front-end for technology-driven programs is the best way to ensure that preventable instances of error and abuse do not hinder important efforts at all levels of government to share information and prevent terrorist attacks.

"New" Technologies

Information technologies are regularly pushed to their limits, stretched and combined to create new technologies and new uses of existing technologies. Many of these new technologies are not easily categorized and thus do not fit easily into existing privacy protection assessments. To the extent that DHS offices have explored such "new" technologies for potential applications, the DHS Privacy Office has ensured that the privacy protection issues are part of any preliminary discussions. Sometimes these discussions take place informally – in discussions among colleagues. At other times, the discussions are much more formal – occurring at workshops and conferences.

In addition to collaboration with DHS offices, the DHS Privacy Office also looks ahead at emerging technologies that may raise privacy protection concerns in the future. This separate research initiative focuses on broad issue-spotting and general preparedness for areas in which privacy and technology may merge to create new challenges to integrating privacy protections with new technology that may be used to further secure the homeland. Some examples of these new "new technologies" are geospatial information systems and services, unmanned aerial technologies and ubiquitous sensor networks. Each of these "forward-edge" technologies, among others, may potentially raise separate privacy protection concerns and, to that extent, the Privacy Office is taking the lead for DHS in reviewing their proposed or hypothetical uses and their impact on individual privacy, actively commenting within DHS and as part of larger discussion groups across the U.S. government on next generation information technologies.

In addition to addressing the privacy protection issues raised by today's technology, the DHS Privacy Office serves DHS offices by scouting issues raised by potential technologies of the future so that if and when those "next" technologies are

[1] http://www.cnet.com/video/webcast/wireless_glossary.html

brought to the Department of Homeland Security, the framework of privacy protections can be addressed up front, rather than after research efforts and expenses are expended.

Regardless of the format, however, the Privacy Office has pursued its mission to ensure that an appreciation of privacy requirements is part of the developmental life cycle of any program, system, or use of technology.

PRIVACY ACT COMPLIANCE

" . . . (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;"

Section 222 (2),
The Homeland Security Act of 2002

The purpose of [the Privacy Act] is to promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.

Senate Report 93-1183,
September 26, 1974

In accordance with Section 222 of the Homeland Security Act of 2002, the Privacy Office ensures that DHS activities comply with the Privacy Act of 1974. Specifically, the Privacy Act requires government agencies to publish notices in the Federal Register upon the establishment or revision of systems of records, to account for disclosures of certain records, and to agree in writing with another agency before entering into a computer matching program,[2] and to provide individuals access to records maintained about them.

Systems of Records

Legacy Systems of Records

The Privacy Office is engaged in taking inventory of all Privacy Act systems of records in order to reorganize and republish them under the DHS umbrella. This is a significant undertaking; close to 200 systems of records have been identified across DHS and its 22 component agencies that pre-existed the creation of the Department of Homeland Security. In the process, the Privacy Office will reorganize and streamline its

systems of records, ensure that the routine uses[3] are consistent and appropriate across the agency, and that each office systematically has procedures in place accounting for data sharing.

New Systems of Records Notices

By the end of December 2003, DHS Headquarters and components had published eight new Privacy Act notices in Volume 68 of the Federal Register at the following cites: 68 Fed. Reg. 45265-01; 68 Fed. Reg. 49496-01; 68 Fed. Reg. 55642-01; and 68 Fed. Reg. 69412-01 and 69414-01.

New notices included an interim final notice for the CAPPS II Program[4] and a notice about a new system of records for SAFETY Act information collected by the Department. They also included republication of three notices by the Transportation Security Administration within DHS and two from the Directorate for Border and Transportation Security which were revised to accommodate the inauguration of the US-VISIT Program on December 12, 2003. Additionally, the Coast Guard announced its Health Information Privacy Program on April 28, 2003, which allows for appropriate uses and disclosures of protected health information concerning members of the Armed Forces.

Many other Privacy Act notices are now being drafted or revised and will be thoroughly reviewed by the Privacy Office to ensure compliance with the Privacy Act, as well as with fair information principles, generally, for the collection of personally-identifiable data.

Accounting for Disclosures

DHS components have in place memoranda of understanding allowing for the regular exchange of law enforcement data with federal and state agencies, such as through the Treasury Enforcement Communications System, as well as routine uses that permit release of Privacy Act data under carefully controlled circumstances to appropriate foreign, federal, state and local agencies. The DHS Privacy Office worked to ensure that all DHS employees remain cognizant of the need to account for any Privacy Act disclosure of records and to promote the use of technology in new record systems to facilitate these accountings in ways that are privacy enhancing.

Matching Agreements

U.S. Citizenship and Immigration Services (CIS) and the Coast Guard have matching agreements. CIS matching agreements involve the SAVE Program, Systematic Alien Verification for Entitlements Program, and facilitate the exchange of information between California, Colorado, New York, New Jersey, the District of Columbia,

---

[2] A "matching program" is a computerized comparison of two or more automated systems of records for the purpose of determining eligibility for a payment under a Federal benefit program or recouping payments already made.

[3] Under the Privacy Act, a "routine use" is the use of a record that is compatible with the purpose for which the record was collected.

[4] The CAPPS II Program has since been replaced by a new program, Secure Flight.

Massachusetts and the Department of Education to verify alien applicant eligibility for Supplemental Security Income, Temporary Assistance for Needy Families, food stamps, Medicaid, unemployment and, in the case of the Department of Education, educational assistance. The Chief Privacy Officer approved a one-year renewal of several matching agreements with the states concerning Social Security and welfare benefits during 2003.

The Coast Guard participates in two matching agreements with the Department of Defense, the Veterans Administration and the Social Security Administration to verify eligibility for supplemental security income payments and special veterans' benefits. These agreements were initiated prior to the establishment of the Department of Homeland Security and are eligible for renewal in 2004.

Requests

Although Privacy Act requests for access to information or redress typically are included in agencies' annual FOIA reports and not separately reported, some DHS components have the capability separately to identify these requests. Based on reports from its components, DHS closed approximately 24,000 Privacy Act requests during fiscal year 2003. The vast majority of these requests were processed by United States Citizenship and Immigration Services which maintains, among other systems of records, the Alien File and Central Index System, consisting of records concerning all persons who are subject to any provision of the Immigration and Nationality Act. These data help to demonstrate that privacy is a core value at the heart of DHS's mission.

LEGISLATIVE AND REGULATORY REVIEWS

"*. . . (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;"*

Section 222 (3), The Homeland Security Act of 2002

The Chief Privacy Officer for DHS is required by statutory mandate to evaluate all legislative and regulatory proposals involving the collection, use and disclosure of personally-identifying information by DHS. Institutional processes within DHS have been established to ensure that this occurs in a systematic fashion.

Legislative Proposals

The Privacy Office works closely with the DHS Office of Legislative Affairs and the Office of the General Counsel to ensure that all bills on which DHS is asked to record its opinion that in any way concern individual privacy matters, the collection of personal information, agency disclosure policies, information sharing with DHS partners, or matters likely to be of significant interest to the international privacy community are reviewed by the Privacy Office. On any typical day, in fact, it is not uncommon for the Privacy Office to provide comments on numerous legislative proposals.

Regulatory Initiative Reviews

Similarly, the Privacy Office works closely with the Office of the General Counsel to ensure that all DHS regulatory initiatives are reviewed for compliance with federal privacy law and DHS policy. No notice of proposed rulemaking that affects the collection of personally identifiable data goes forward for Federal Register publication without concurrence by the Privacy Office. Moreover, the Privacy Office has instituted policies to ensure that Privacy Impact Assessments, which are required by the E-Government Act of 2002, are published in the Federal Register and are made available prior to or in connection with the publication of notices of proposed rulemaking that cover the applicable programs.

The influence of the Privacy Office on regulatory developments is illustrated by the regulatory history of the CAPPS II Program. While still a part of the Department of Transportation, the Transportation Security Administration proposed a new system of records under the Privacy Act for "Passenger and Aviation Security Screening Records" in January 2003, prior to the installation of the Chief Privacy Officer for DHS. After the Chief Privacy Officer assumed her responsibilities, however, the proposed system notice for these records was significantly and substantially revised, in large part due to the public comments received on the initial notice, and a new notice, including a request for additional public comments, was published on August 1, 2003. That notice indicated that a further Privacy Act notice would be published in advance of any active implementation of the CAPPS II system, a decision made at the direction of the DHS Privacy Office. (See Appendix G)

In 2004, the Department announced a new domestic automated passenger prescreening program, Secure Flight. The new program is designed to more accurately authenticate the identity of travelers and to screen appropriately for heightened risks for terrorism. The Privacy Office anticipates that going forward it will continue to exercise close oversight over the final parameters of Secure Flight to ensure that robust privacy protections are fully implemented in the system architecture.

Congressional Testimony

On February 10, 2004, the Chief Privacy Officer testified before the Subcommittee on Commercial and Administrative Law of the Judiciary Committee of the U.S. House of Representatives regarding the activities of the Privacy Office. Ms. O'Connor Kelly outlined the Department of Homeland Security's commitment to privacy protection, the establishment of the Privacy Office, the key frameworks enforced by the Privacy Office, the challenge of operationalizing privacy throughout DHS through best practices and consistent policies and education efforts, public outreach, policy challenges, and the need to balance transparency and security operations. (See Appendix E) In addition to this testimony, the DHS Privacy Office frequently reviews the Congressional testimony of other DHS representatives to ensure consistency in DHS statements on the importance of privacy to the agency's mission.

PRIVACY IMPACT ASSESSMENTS

". . . (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;"

Section 222 (4), The Homeland Security Act of 2002

"Privacy Impact Assessments are a new and important tool in the tool belt of privacy practitioners across the federal government."

Nuala O'Connor Kelly, Chief Privacy Officer
Speech to Heritage Foundation, November 17, 2003.

In accordance with Section 208 of the E-Government Act of 2002, the Department of Homeland Security is required to issue Privacy Impact Assessments (PIAs) when the agency substantially modifies existing information technology systems or creates new information technology systems that contain personally identifiable information. The purpose of a PIA is to ensure that information technology systems of the Federal Government are maintained in conformity with fair information principles concerning notice, consent, access, redress, data integrity and security.

Separately, Section 222 of the Homeland Security Act of 2002 requires the Chief Privacy Officer for DHS to require and review PIAs for proposed rules of the agency.

A PIA must address at least two issues:

1. It must determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.

2. It must evaluate the protections and alternative processes for handling information to mitigate potential privacy risks.

A PIA outlines salient points about new or existing information technology systems by answering questions about the information that will be collected, the opportunity individuals will have to redress information collected about themselves, who will be able to access the information, how the system and data will be maintained, what administrative controls will be in place, and how the decision to use a system was made.

The Privacy Office has been instrumental in making the PIA process a focal point for privacy activities at DHS. By providing written and oral training in addition to specific guidance materials, the Privacy Office has enabled all DHS program offices to incorporate privacy into their fundamental program planning.

The effective date of the PIA requirement roughly coincided with the establishment of the DHS Privacy Office. This confluence of events allowed the Chief Privacy Officer

the opportunity both to provide DHS input into the final OMB guidance and to ensure that the PIA process became firmly embedded in the Department of Homeland Security.

From the initial drafting of a PIA to the final product, the Privacy Office has provided PIA leadership to DHS offices and components. A Privacy Office publication, *PIAs Made Simple*, is in use throughout the agency, and several PIAs for major DHS initiatives have set the standard for agency documents of this kind.

In addition to PIA development for programs since April 2003, the Privacy Office has reviewed nearly 90 PIAs in connection with the OMB 300 process, which requires privacy impact assessments in connection with any funding request of more than $500,000 for new technologies or improvements on existing information systems and technologies. Additionally, the Privacy Office is reviewing PIAs, or advising on the need for their development, in connection with DHS rulemakings. Finally, as a policy matter, the Privacy Office may request that a DHS office or component undertake the preparation of a PIA to assist with a privacy review of a non-IT or rule-based proposal for a DHS program.

The Chief Privacy Officer provides final agency review of PIAs before they are forwarded to the Office of Management and Budget and then published in the Federal Register, or otherwise made publicly available. The Privacy Office has provided critical privacy advice to new DHS initiatives, resulting in changes in many cases that will improve privacy protections in DHS programs. Procedures are now well established to ensure that privacy is considered throughout the lifecycle of DHS processes and programs and that fair information principles inform policy decisions concerning data collection and use.

PRIVACY COMPLAINTS

" . . . (5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters."

Section 222(5), The Homeland Security Act of 2002

The Privacy Office has examined privacy practices at the Department in a variety of ways, including through the lens of complaints. This review has encompassed alleged systemic violations of privacy and more particular violations concerning particular individuals.

JetBlue Data Transfer

An alleged privacy violation involving the Transportation Security Administration was brought to the attention of the Privacy Office in September 2003. The potential violation involved the transfer of Passenger Name Records (PNRs) from JetBlue Airways to the Department of Defense, a transfer that was facilitated by certain personnel of the Transportation Security Administration. While the time of the potential violation predated the creation of the Department of Homeland Security, the matter raised serious concerns about the proper handling of personally identifiable information by government employees now within DHS.

In addressing the potential privacy violation, the Privacy Office thoroughly analyzed the matter, ultimately deciding that a Privacy Act violation had not occurred. The Privacy Officer found, nevertheless, that prophylactic action was required. Consequently, the Privacy Office made several recommendations regarding the need for privacy training for TSA employees as well as for DHS employees generally, the need to establish guidelines for data sharing, the need to have in place stronger controls for private-sector data sharing and the need to have the Inspector General review the matter to determine if further IG action is required. The Privacy Office report on the transfer of JetBlue PNR data is available to the public on the DHS website.

http://www.dhs.gov/interweb/assetlibrary/PrivacyOffice_jetBlueFINAL.pdf

Other Airline Data Transfers

Subsequent to the JetBlue report, the Privacy Office was alerted to the fact that additional PNR transfers had taken place with the involvement of TSA. Accordingly, the Privacy Office is now reviewing these additional transfers to ascertain if they were accomplished in compliance with applicable privacy laws and regulations. A further public report is anticipated as a result of this investigation.

Matrix

Another example of the Privacy Office's investigatory efforts in response to privacy complaints involves the MATRIX program (Multi-State Anti-Terrorist Information Exchange), a system of integrated law enforcement and commercial databases that has been funded through a cooperative agreement with the DHS Office of Domestic Preparedness. From its inception, the system has been subjected to a substantial number of complaints and inquiries to the Privacy Office.

In response to these requests and ongoing concerns from various segments of the public, the Privacy Office has undertaken a full-scale review of the MATRIX program, seeking to gain an understanding of its components and functions and the role of the Department in supporting it. The results of that review will be made public in the near future through a forthcoming report.

CAPPS II

From April 2003 until the present, the Privacy Office received thousands of contacts, most via e-mail and many in identical form, expressing concerns with respect to the proposed CAPPS II program. Much of the correspondence came in the form of public comment to privacy notices on the proposed program that were published in the Federal Register, seeking such comments. E-mail correspondence received automatic acknowledgements of receipt. The Chief Privacy Officer reviewed the contacts with the office and took the concerns expressed into consideration in formulating internal privacy guidance to program managers and DHS leadership. Additionally, the Chief Privacy Officer had numerous discussions with privacy advocates and other private sector representatives concerning the program's development about the need to address privacy concerns.

Many of the CAPPS II complaints centered on fears that the program would be a broad surveillance program that targeted innocent citizens and travelers, rather than narrowly tailored to potential terrorists. Other complaints expressed concern about the use of private sector data sharing with DHS in a manner that might lead to discriminatory treatment based on data, the integrity of which could not be verified and concerns that the data might not be covered by Privacy Act protections. Still others complained about lack of notice on the program details and what appeared to be a lack of robust access and redress rights for individuals.

International Privacy Complaints

Fewer than a dozen pieces of correspondence were received by the Privacy Office at the Departmental level relating to international inquiries about DHS programs or information that DHS may have collected about an individual on travel to or through the United States. Most of the matters were requests for the an individual's personal information held by DHS, what exactly was collected in connection with airline flights, how was it used and for what period would such information be retained – whether Passenger Name Record information or Advance Passenger Information System (APIS) information. Included in these contacts were several letters from members of the European

Parliament, one from a European Data Protection Commissioner on behalf of a European citizen, one from a Canadian Data Protection Commissioner requesting information on the impact of the Patriot Act and privacy protections for Canadian personal data outsourced to a U.S. company, and several letters from individuals believing that they were on a No-Fly List or seeking confirmation that they were not. After reviewing the issues raised, the Privacy Office provided appropriate responses in each case.

INTERNAL EDUCATION; EXTERNAL OUTREACH

"The role of a privacy officer . . . is simultaneously both within and without the organizational structure and culture . . . we are educators and leaders and communicators within, and effective liaisons and open doors to those outside."

Nuala O'Connor Kelly
Speaking to the International Association of Privacy Professionals, October 30, 2003

Education and Training

One way to ensure that privacy is embedded into the culture of the Department of Homeland Security is through a vigorous education and training program. The Privacy Office recognizes the value and need for systematic privacy training at the Department and has spent the last fourteen months creating the framework for a comprehensive program.

Many of the agencies that merged with the Department had their own training initiatives and so the Privacy Office's work has included a survey of existing resources to ascertain how they might be leveraged for general Departmental use. In 2004, a Director of Privacy Compliance was hired to serve as the focal point of training and compliance initiatives.

The Privacy Office is now creating and implementing privacy awareness training for all DHS employees and new hires. The primary goal of privacy awareness training is to ensure that DHS employees are fully informed about how to handle personally-identifiable information in a responsible and appropriate manner. This program will not only be a requirement for all employees, but it will also set the baseline for subsequent awareness and communication campaigns by the Privacy Office. Subsequent training modules are planned that will be tailored to individual groups within DHS to ensure a broad agency understanding of how privacy integrates with specific DHS programs so that it is addressed appropriately.

DHS Privacy Advisory Committee

As important as internal training initiatives are for DHS employees in order to foster an appreciation of privacy, equally important for the mission of DHS and for the Privacy Office is outreach, to bring in new ideas from outside the agency in order to provide for better informed decisions. One means of outreach that promises to be especially beneficial to the Privacy Office and to DHS is the Data Integrity, Privacy, and Interoperability Advisory Committee. The Committee will advise the Secretary and the Chief Privacy Officer on programmatic, policy, operations, administrative, and technological issues that affect individual privacy, as well as on data integrity and data interoperability and other privacy-related issues.

The Privacy Office solicited applications for the advisory committee in 2004. (See Appendix I) The Committee will be appointed by the Secretary and must be qualified to

serve by virtue of the education, training, or experience. The panel will include recognized experts in the fields of data protection, privacy, interoperability, and emerging technologies. Membership terms will be for a period of up to four years, with initial terms staggered to permit continuity and orderly turnover.

There is significant interest in this advisory committee; as of the date of this report, the Privacy Office received more than 125 applications for positions from a wide variety of qualified individuals. The Privacy Office intends to build a balanced but diverse advisory committee.

THE DEPARTMENTAL DISCLOSURE PROGRAM: IMPLEMENTING THE FREEDOM OF INFORMATION ACT

"Secretary Ridge has said that "fear of government abuse of information . . . is understandable, but we cannot let it stop us from doing what is right and responsible." The antidote to fear, as he has said, "is an open, fair, and transparent process that guarantees the protection and the privacy of that data." I commit to this Committee, to the American people whom we serve, and to our neighbors around the globe, that the Privacy Office is implementing this philosophy on a daily basis at the Department of Homeland Security."

Nuala O'Connor Kelly
Testimony before the House of Representatives
Committee on the Judiciary, Subcommittee on
Commercial and Administrative Law, February 10, 2004

In the first year of the Department of Homeland Security's inception, its Freedom of Information Act (FOIA) program has evolved to become an integral part of DHS operations.

Armed with interim FOIA rules a management directive outlining FOIA responsibilities for all DHS offices, and a statutory framework of broad agency disclosure mandated by FOIA itself, the Privacy Office provides overall policy guidance to more that 430 FOIA and Privacy Act personnel agency-wide. A Departmental Disclosure Officer, reporting directly to the Chief Privacy Officer manages this function.

The Departmental Disclosure Officer accepts all requests for records submitted pursuant either to the FOIA or the Privacy Act of 1974 for DHS Headquarters elements, consisting of the Offices of the Secretary and Deputy Secretary, Legislative Affairs, Public Affairs, Chief Financial and Information Officers, Private Sector, International Affairs, Counter Narcotics and State and Local Coordination, and the Management Directorate. Additionally, the Departmental Disclosure Officer serves as a conduit to DHS Directorates and component agencies, forwarding them FOIA and Privacy Act requests seeking records they maintain.

The DHS Directorates -- Science and Technology, Information Analysis and Infrastructure Protection, Border and Transportation Security, and Emergency Preparedness and Response – have their own separate FOIA personnel. Additionally, DHS components such as the United States Secret Service, the Coast Guard, U.S. Citizenship and Immigration Services, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement, employ FOIA officers and information specialists.

The DHS website, http://www.dhs.gov, contains information about the FOIA process to assist members of the public seeking to obtain records from DHS. The website includes instructions on where to send a FOIA request, the requirements for submitting a

FOIA request, and an estimate of how long it will take for DHS to respond to a FOIA request.

During fiscal year 2003, personnel working under the umbrella of DHS processed 160,902 FOIA requests (agencies that preexisted the creation of DHS merged on March 1, 2003). Seventy-two percent of these requests were answered with either a full release of records or a partial release, with the most common reasons for withholding information being privacy-related (Exemptions 6 and 7(C)) of the FOIA were used nearly 62,000 times). A more complete picture of FOIA operations at DHS is presented in the DHS Annual FOIA Report, which can be found on the Internet at: http://www.dhs.gov/interweb/assetlibrary/FOIADHSFY2003AnnualReport.pdf. (See Appendix J)

IMPLEMENTING PRIVACY OVERSIGHT

Most of the agencies that merged with the Department of Homeland Security had personnel already in place to handle Privacy Act and FOIA matters, and these key staff have become part of a unified team of professionals dedicated to ensuring government transparency and privacy compliance. At the same time, the Privacy Office recognized that certain programs, because of their high visibility and impact, require the services of a designated Privacy Officer to ensure that personally-identifiable information, which is required for program operations, is collected and maintained in strict compliance with fair information principles.

Privacy Officers have been appointed for the US-VISIT Program, the Transportation Security Administration, which oversees a multitude of programs affecting the traveling public, and the National Cyber Security Division, which has programs that push the cutting edge of technology and thus have the potential significantly to affect privacy. These privacy officers report to the Chief Privacy Officer and to their organizations. They work closely with the DHS Privacy Office and their respective programs on a wide variety of privacy issues and initiatives, including development of PIAs, privacy policies, and privacy notices to inform the public about these DHS initiatives, to name a few. The impact of a dedicated Privacy Officer within these program and component areas is easily seen by reviewing their privacy accomplishments this past year.

The US-VISIT Program's Privacy Accomplishments

The US-VISIT Program represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity back to our immigration and border management systems. It is also leading the way for incorporating biometrics into international travel security systems.

When fully implemented, US-VISIT will provide a dynamic, interoperable information system involving numerous stakeholders across the government. US-VISIT began implementing Increment 1, collecting and retaining covered foreign visitor's biographic, travel, and biometric information (inkless digital index finger scans and digital photographs), on January 5, 2004, at 115 air and 14 seaports.

The US-VISIT Privacy Officer, who can be reached at usvisitprivacy@dhs.gov, is accountable for compliance with applicable privacy laws, regulations, and US-VISIT privacy requirements. Working with the DHS Privacy Office, the Privacy Officer is also responsible for creating and sustaining a culture within the US-VISIT program office, where privacy is paramount and fully integrated into the business and technology planning and development processes.

In close consultation and coordination with the Chief Privacy Officer, US-VISIT published a privacy policy on November 21, 2003, which can be found at http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf. The privacy policy explains the purpose of the program, who is affected, what information is collected, how

the information is used, who has access, how the information is protected, how long the information is retained, how to have inaccurate information corrected, and who to contact for more information. US-VISIT developed the privacy policy to help address critical privacy questions and concerns.

Although US-VISIT derives its capability from the integration and modification of existing systems of records, it nevertheless represents a new business process that involves new uses of existing data and the collection of new data items. As a result, and in an effort to make the program transparent as well as to address any privacy concerns that may arise as a result of the program, the Chief Privacy Officer worked with US-VISIT to perform a PIA in accordance with the guidance issued by OMB on September 26, 2003.

The US-VISIT PIA was published on January 4, 2004, and is available at www.dhs.gov/us-visit. The PIA was hailed by many in the privacy community as an excellent model of transparency because it includes detailed information about the program, the technology and the privacy protections. (See Appendix F) The DHS Chief Privacy Officer and the US-VISIT Privacy Officer have met with numerous advocacy, privacy and immigration groups to solicit input and hear concerns. These concerns and recommendations have been taken into account in the development of the program and will be incorporated into future updates to the PIA as US-VISIT is further developed.

US-VISIT has established the basic organizational elements for its privacy program and now is in the process of defining roles and responsibilities and effective organizational interaction with key stakeholders. Going forward, US-VISIT intends to develop oversight and measurement capabilities, including a privacy compliance audit process to check progress towards meeting privacy goals.

In addition to the close working relationship maintained with the DHS Privacy Office, the US-VISIT Privacy Officer reports to the US-VISIT chief strategist in order to ensure that the privacy principles are applied to policies, standards, procedures, and guidelines. This is accomplished by developing and implementing requirements for privacy-compliant activities and operations including data usage agreements between US-VISIT and other agencies authorized to have access to US-VISIT data. Privacy principles are imbedded in the systems development and security architecture through administrative, procedural, physical, and electronic safeguards that control privacy risk. Awareness programs have also been instituted to make agencies, vendors, foreign visitors, and the public aware of the US-VISIT privacy principles and practices. Program monitoring and compliance auditing is being conducted to ensure adherence to the privacy principles, laws, regulations, and requirements.

US-VISIT has implemented a three-stage process for individuals to inquire about the data US-VISIT has collected in order to facilitate the amendment or correction of data that are not accurate, relevant, timely, or complete. The first stage in the process occurs at the primary inspection lane and provides on-the-spot data correction. A U.S. Customs and Border Protection Officer has the ability to manually correct the traveler's name, date of birth, flight information, and country-specific document number and document type errors. For data mismatches involving biometrics, the officer sends a data correction request to US-VISIT. The second stage allows for visitors processed through US-VISIT to have their records reviewed for accuracy, relevancy, timeliness, or completeness.

The US-VISIT Privacy Officer has set a goal of processing redress requests within 20 business days. Individuals who are not satisfied with the result can progress to the third stage by appealing to the DHS Chief Privacy Officer who will conduct an investigation and provide final adjudication. With nearly six million travelers processed through US-VISIT to date, only 31 individuals have inquired about their US-VISIT records. All of those inquires have been addressed and resolved by the US-VISIT Privacy Officer.

TSA's Privacy Accomplishments

The TSA Privacy Officer, whose responsibilities consist of implementing the policies and directives of the DHS Chief Privacy Officer, began oversight activities of TSA programs in March 2004. Since that time, working in close coordination with the DHS Privacy Office, the TSA Privacy Officer has assumed an active -- and in fact, proactive -- role in ensuring that TSA programs are fully consonant with all privacy requirements.

For example, the TSA Privacy Officer has been closely involved in the planning and development of TSA programs that require the collection, use and disclosure of personal information, ensuring that the information collected is: (1) necessary; (2) properly stored; (3) securely transmitted; (4) disclosed only to those individuals with a "need to know;" and (5) that there are sufficient redress mechanisms in place for those individuals who are affected by the collection. Some of these programs include the Registered Traveler Pilot Program and the screening program for holders of licenses for transport of hazardous materials.

TSA has developed training materials for employees on various aspects of the Privacy Act as well as on TSA privacy policies that are applicable to every functional level of the agency. For example, in cooperation with the DHS Privacy Office, TSA developed training materials on the Privacy Act describing each employee's responsibilities with respect to the collection, use and disclosure of individuals' personally-identifiable information. This training, entitled "Respecting Privacy, Preserving Freedoms," is required for all TSA employees both at headquarters and in the field. Additional training is also being developed that will focus on DHS privacy policies and their applicability to the employee's job description.

TSA held a successful Privacy Week in spring 2004, at which all employees received mandatory privacy awareness training. Senior management from DHS and within TSA strongly supported the initiative.

The TSA Privacy Officer, working closely with the Chief Privacy Officer and Privacy Office staff, also has exercised strong leadership in ensuring the TSA programs complete and publish Privacy Impact Assessments related to various programs that are currently in prototype phase or have are being implemented. PIAs for the following programs have been completed:

(a) Security Threat Assessments for Commercially Licensed Drivers with HAZMAT Endorsements (April 15, 2004; revised June 1, 2004)

(b) Registered Traveler Prototype (June 24, 2004)

(c) Airport Access Control Pilot Project (June 18, 2004)

(d) Security Threat Assessment for SIDA and Sterile Area Workers (June 15, 2004)

The above-mentioned Privacy Impact Assessments have been published and can be found on the DHS Chief Privacy Officer's website (www.dhs.gov\privacy). A number of other Privacy Impact Assessments are currently in progress and will be published by the end of the year.

The TSA Privacy Officer also is involved in other initiatives intended to ensure that privacy is at the core of TSA's mission. For example, TSA currently is reviewing data sharing with contractors, law enforcement, airlines and all other relevant parties inside and outside the agency in order to develop appropriate policies and employee guidance.

National Cyber Security Division – US-CERT Privacy Accomplishments

The National Cyber Security Division (NCSD) has worked diligently during the last year, most notably through the leadership of its Privacy Officer, to help further the mission of the DHS Privacy Office in the context of the mission of the NCSD. The NCSD is tasked by the Secretary with the overarching responsibility to coordinate the implementation of the *National Strategy to Secure Cyberspace* and, consistent with the mandate of Homeland Security Presidential Directive 7, to serve as a focal point for the public and private sectors for cyber security. As detailed in the *Strategy*, our nation has become increasingly dependent on cyberspace for our national security, our economic well-being, and our law enforcement and public safety. With the increasing migration of personal information onto the interconnected network of information systems in the public and private sectors, it is more important than ever that we enhance the security of cyberspace to protect the privacy of all individuals.

NCSD is working to fully understand the privacy implications of its mandate and be cognizant of the possible impact on privacy of the implementation of its mission. In furtherance of its mandate, NCSD facilitates interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.

The NCSD operational arm is the U.S. Computer Emergency Readiness Team (US-CERT), a partnership between the NCSD and the private sector that was established to help protect and maintain the continuity of the Internet and our nation's cyber infrastructure. The overarching approach to this task is to facilitate and systemize global and domestic coordination of preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States. To this end, while endeavoring to scrupulously respect privacy rights and obligations, US-CERT is building a robust cyber watch and warning capability, launching a public-private partnering effort to build

situational awareness and cooperation, and coordinating with Federal agencies, state and local governments, and the private sector. The overarching goal is to enhance America's ability to predict, prevent, respond to, and recover from cyber attacks and incidents, and the cyber consequences of physical attacks and incidents.

Operationally, NCSD-US-CERT has a privacy policy for the US-CERT website and is developing a privacy policy for the US-CERT HSIN Portal that is a secure collaboration vehicle in a pilot phase. NCSD also is working with the Privacy Office on privacy issues related to cyberspace situational awareness.

THE WAY FORWARD:

A PERSONAL NOTE FROM THE CHIEF PRIVACY OFFICER

America, it has been said, is a country of "rugged individualists." We asked in our Declaration of Independence that our government be a "new guard for future security," while at all times respecting the primacy of the individual's rights. Our Constitution, while not specifying a right to privacy, reflects the universal recognition that privacy is an important right, such that legal scholars recognize privacy as a "penumbral" Constitutional right. Our forefathers recognized that to have security, but not privacy, is insufficient. We share that recognition today.

Reflecting this philosophy, the Department of Homeland Security is not only a counterterrorism agency, but also, as Secretary Ridge has emphasized so often, a protective agency. The senior leaders of this Department, with whom I am proud to serve, are committed to safeguarding the people and places of our country, as well as our liberties and our way of life. A significant part of safeguarding those liberties is protecting the dignity and the uniqueness of the individual. And protecting the dignity and uniqueness of the individual requires -- indeed demands -- that we protect the privacy of that individual. It therefore has been my honor during the first year of the Department of Homeland Security's existence to help ensure that we protect the privacy of each individual, because I, like my colleagues in the Department of Homeland Security, recognize the absolute imperative to foster security while protecting individual privacy.

I close this report recognizing that we live in uncertain times. It causes me to consider a lesson from Thomas Jefferson, who noted, "It is part of the American character… to surmount every difficulty with resolution . . . ." With resolution and pragmatic optimism we will continue the crucial work of this Department and of the Privacy Office: to protect America and its many freedoms -- including individual privacy.

Thank you for the opportunity to serve and to report on privacy activities at the Department of Homeland Security.

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, District of Columbia
July 2004